

CLAIMS

1 1. A computer implemented method for gleaning file
2 attributes independently of file format, the method
3 comprising the steps of:
4 a non-application specific file attribute manager
5 receiving a plurality of files in a
6 plurality of formats;
7 the file attribute manager scanning the plurality
8 of received files in the plurality of
9 formats;
10 the file attribute manager gleaning attributes
11 concerning each of the plurality of scanned
12 files in the plurality of formats;
13 the file attribute manager storing gleaned
14 attributes concerning each of the plurality
15 of scanned files as records in a database;
16 and
17 the file attribute manager indexing attributes
18 being stored as a record in the database
19 concerning a specific file according to
20 contents of that file.

1 2. The method of claim 1 wherein:

2 the specific gleaned attributes concerning a
3 specific file are a function of a protocol
4 according to which the file is transmitted.

1 3. The method of claim 1 wherein:
2 the specific gleaned attributes concerning a
3 specific file are a function of the format
4 of that file.

1 4. The method of claim 1 further comprising:
2 the file attribute manager indexing attributes
3 being stored as a record in the database
4 concerning a specific file according to a
5 secure hash of the contents of that file.

1 5. The method of claim 1 further comprising:
2 the file attribute manager indexing attributes
3 being stored as a record in the database
4 concerning a specific file according to a
5 cyclical redundancy check of the contents of
6 that file.

1 6. The method of claim 1 further comprising:
2 the file attribute manager receiving a plurality
3 of copies of the same file; and

4 the file attribute manager storing a separate
5 record for each received copy of the file,
6 each record being indexed according to the
7 contents of the file, such that each record
8 can be accessed by the single index.

1 7. The method of claim 1 further comprising:
2 deleting records from the database after the
3 records have been stored for a specific
4 period of time.

1 8. The method of claim 1 wherein the non-application
2 specific file attribute manager is incorporated into at
3 least one of the following:
4 a firewall;
5 an intrusion detection system;
6 an intrusion detection system application proxy;
7 a router;
8 a switch;
9 a standalone proxy;
10 a server;
11 a gateway;
12 an anti-virus detection system;
13 a client.

1 9. A computer readable medium containing a computer
2 program product for gleaning file attributes independently
3 of file format, the computer program product comprising
4 program code for:

5 receiving a plurality of files in a plurality of
6 formats;
7 scanning the plurality of received files in the
8 plurality of formats;
9 gleaning attributes concerning each of the
10 plurality of scanned files in the plurality
11 of formats;
12 storing gleaned attributes concerning each of the
13 plurality of scanned files as records in a
14 database; and
15 indexing attributes being stored as a record in
16 the database concerning a specific file
17 according to contents of that file.

1 10. The computer program product of claim 9 further
2 comprising:

3 program code for gleaning specific attributes
4 concerning a specific file as a function of
5 a protocol according to which the file is
6 transmitted.

1 11. The computer program product of claim 9 further
2 comprising:
3 program code for gleaning specific attributes
4 concerning a specific file as a function of
5 the format of that file.

1 12. The computer program product of claim 9 further
2 comprising:
3 program code for indexing attributes being stored
4 as a record in the database concerning a
5 specific file according to a secure hash of
6 the contents of that file.

1 13. The computer program product of claim 9 further
2 comprising:
3 program code for indexing attributes being stored
4 as a record in the database concerning a
5 specific file according to a cyclical
6 redundancy check of the contents of that
7 file.

1 14. The computer program product of claim 9 further
2 comprising:

3 program code for receiving a plurality of copies
4 of the same file; and
5 program code for storing a separate record for
6 each received copy of the file, each record
7 being indexed according to the contents of
8 the file, such that each record can be
9 accessed by the single index.

1 15. The computer program product of claim 9 further
2 comprising:

3 program code for deleting records from the
4 database after the records have been stored
5 for a specific period of time.

1 16. A computer system for gleaning file attributes
2 independently of file format, the computer system
3 comprising:

4 a reception module, configured to receive a
5 plurality of files in a plurality of
6 formats;
7 a scanning module, configured to scan the
8 plurality of received files in the plurality
9 of formats, the scanning module being
10 communicatively coupled to the reception
11 module;

12 a gleaning module, configured to glean attributes
13 concerning each of the plurality of scanned
14 files in the plurality of formats, the
15 gleaning module being communicatively
16 coupled to the scanning module;
17 a storage module, configured to store gleaned
18 attributes concerning each of the plurality
19 of scanned files as records in a database,
20 the storage module being communicatively
21 coupled to the gleaning module; and
22 an indexing module, configured to index
23 attributes being stored as a record in the
24 database concerning a specific file
25 according to contents of that file, the
26 indexing module being communicatively
27 coupled to the storage module.

1 17. The computer system of claim 16 wherein:
2 the gleaning module is further configured to
3 glean specific attributes concerning a
4 specific file which are a function of a
5 protocol according to which the file is
6 transmitted.

1 18. The computer system of claim 16 wherein:

2 the gleaning module is further configured to
3 glean specific attributes concerning a
4 specific file which are a function of the
5 format of that file.

1 19. The computer system of claim 16 wherein:
2 the indexing module is further configured to
3 index attributes being stored as a record in
4 the database concerning a specific file
5 according to a secure hash of the contents
6 of that file.

1 20. The computer system of claim 16 wherein:
2 the indexing module is further configured to
3 index attributes being stored as a record in
4 the database concerning a specific file
5 according to a cyclical redundancy check of
6 the contents of that file.

1 21. The computer system of claim 16 wherein:
2 the reception module is further configured to
3 receive a plurality of copies of the same
4 file; and
5 the storage module is further configured to store
6 a separate record for each received copy of

7 the file, each record being indexed
8 according to the contents of the file, such
9 that each record can be accessed by the
10 single index.

1 22. The computer system of claim 16 further
2 comprising:

3 a deletion module, configured to delete records
4 from the database after the records have
5 been stored for a specific period of time,
6 the deletion module being communicatively
7 coupled to the storage module.

1 23. The method of claim 1 further comprising:
2 examining a file, the file having been processed
3 by the non-application specific file
4 attribute manager;
5 retrieving at least one stored record concerning
6 the file from the database;
7 analyzing gleaned attributes concerning the file,
8 the gleaned attributes having been retrieved
9 from at least one record concerning the file
10 in the database; and
11 responsive to analyzing the gleaned attributes,
12 determining a status concerning the file.

1 24. The method of claim 23 further comprising:
2 responsive to determining the status of the
3 received file to be malicious, blocking the
4 file.

1 25. The method of claim 23 further comprising:
2 responsive to determining the status of the
3 received file to be legitimate, not blocking
4 the file.

1 26. The method of claim 23 further comprising:
2 applying at least one rule specifying how to use
3 gleaned file attributes to process the file.

1 27. The method of claim 26 further comprising:
2 determining at least one of a plurality of rules
3 to apply specifying how to use gleaned file
4 attributes to process the file.